FAA
FEDERAL AVIATION ADMINISTRATION

A New Look at Cyber Defense

October 2003

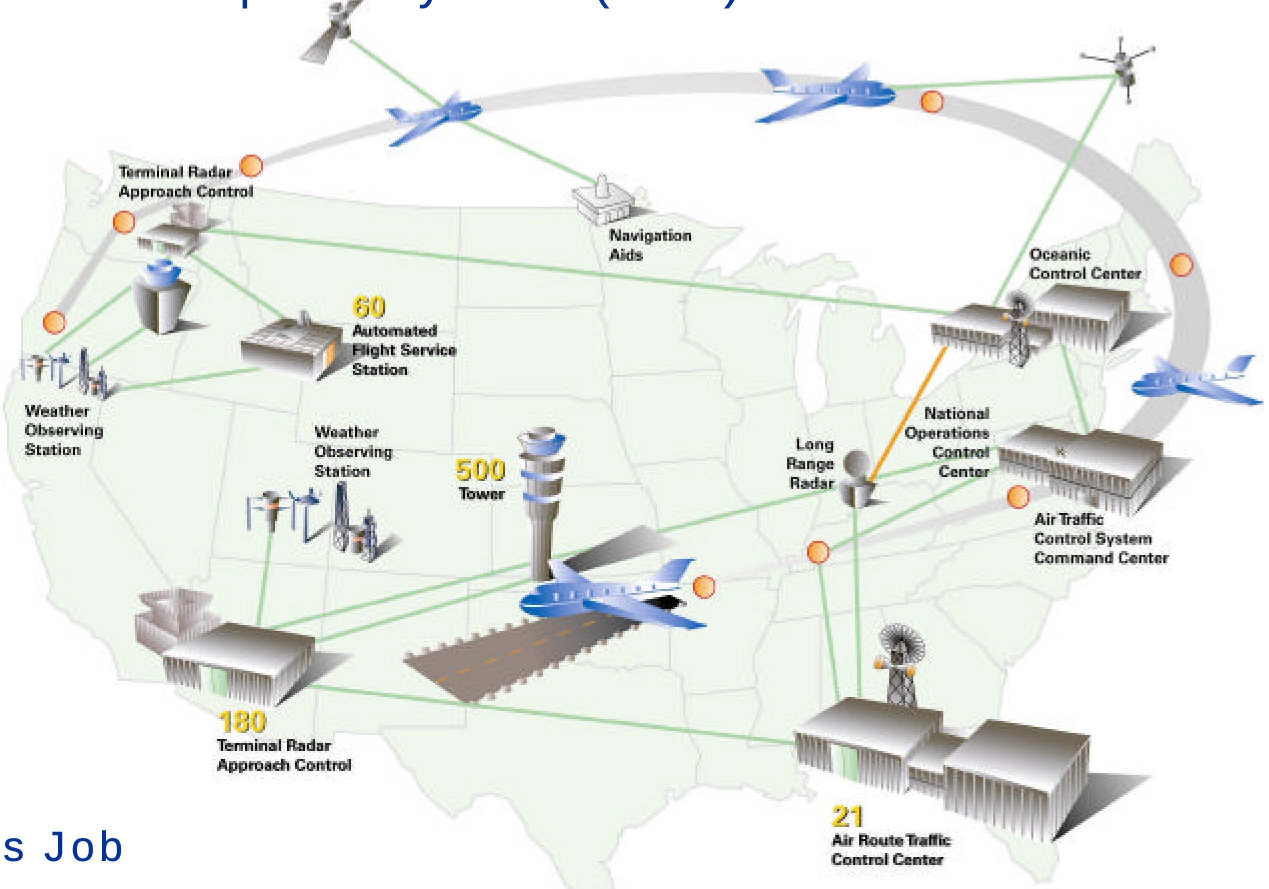
Dan Mehan, Ph.D.
Assistant Administrator for
Information Services and
Chief Information Officer

Background

The slides that follow are an amalgam of two recent presentations given by Dr. Mehan at cyber security conferences:

- Cyber Defense—The Confluence of Operations Research and Computer Security, given at the National Science Foundation Cyber Trust Meeting, August 2003, John Hopkins University; and
- A New Look at Cyber Defense—Blending Insights from Computer Science, Health Science, and Operations Research, given at the American National Standards Institute's Annual Conference, October 2003, Washington, D.C.

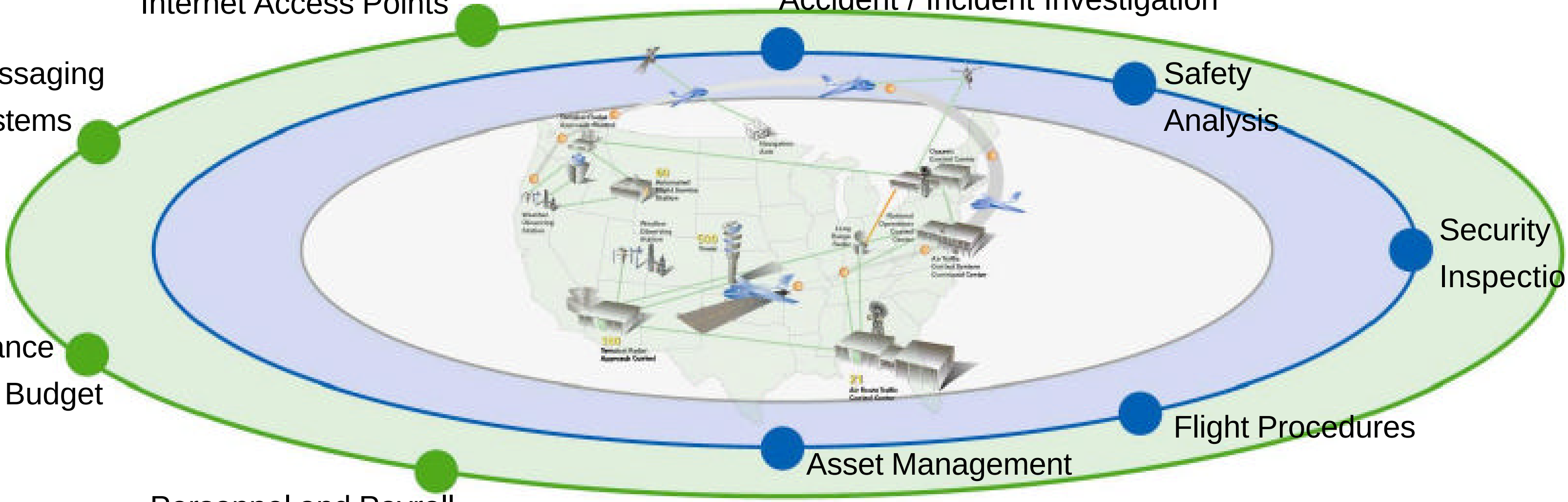
National Airspace System (NAS)


Terminal Radar Approach Control
Navigation Aids
60 Automated Flight Service Station
Oceanic Control Center
Weather Observing Station
Weather Observing Station
500 Tower
Long Range Radar
National Operations Control Center
Air Traffic Control System Command Center
180 Terminal Radar Approach Control
21 Air Route Traffic Control Center

FAA's Job

- Manage more than 30,000 commercial flights to move 2,000,000 passengers safely each day
- Support more than 35,000 general aviation flights on a daily basis
- Regulate and certify the people and aircraft that use our airspace

System of Systems



Internet Access Points

Accident / Incident Investigation

Messaging Systems

Safety Analysis

Security Inspection

Finance and Budget

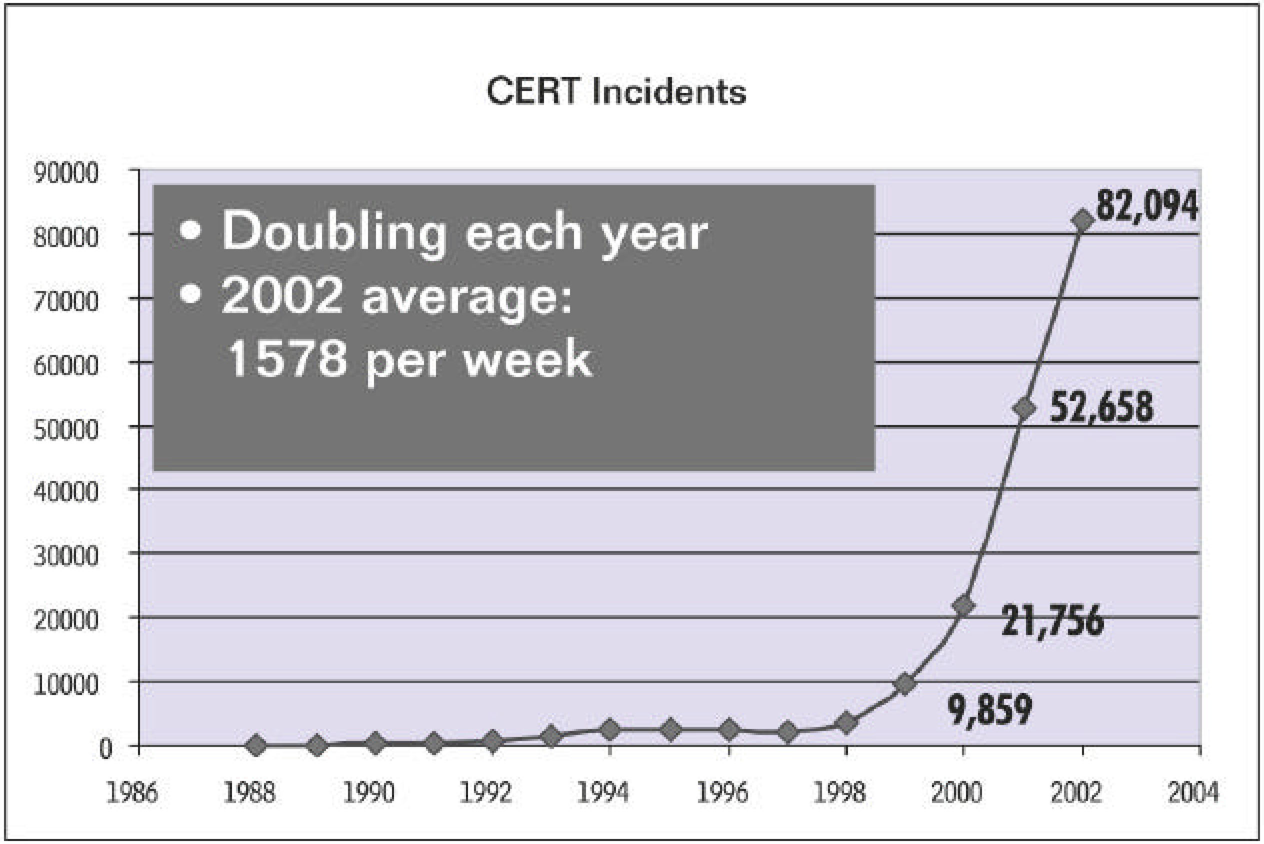
Flight Procedures

Asset Management

Personnel and Payroll

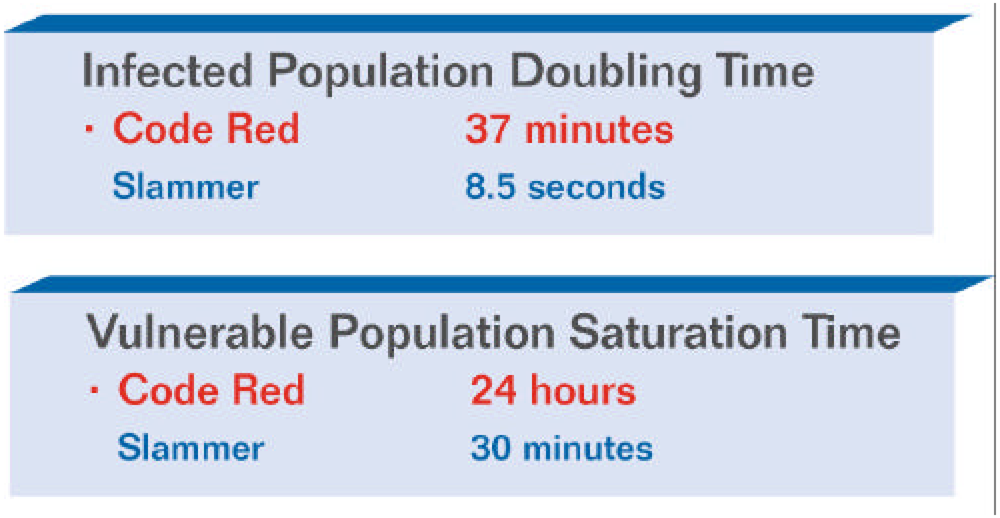
- National Airspace System
- Mission Support
- Administrative

Increasing Number of Incidents Reported to CERT from all Industry and Government Sources



- Doubling each year
- 2002 average: 1578 per week

Increasing Virus Propagation Speed



Infected Population Doubling Time

· Code Red	37 minutes
Slammer	8.5 seconds

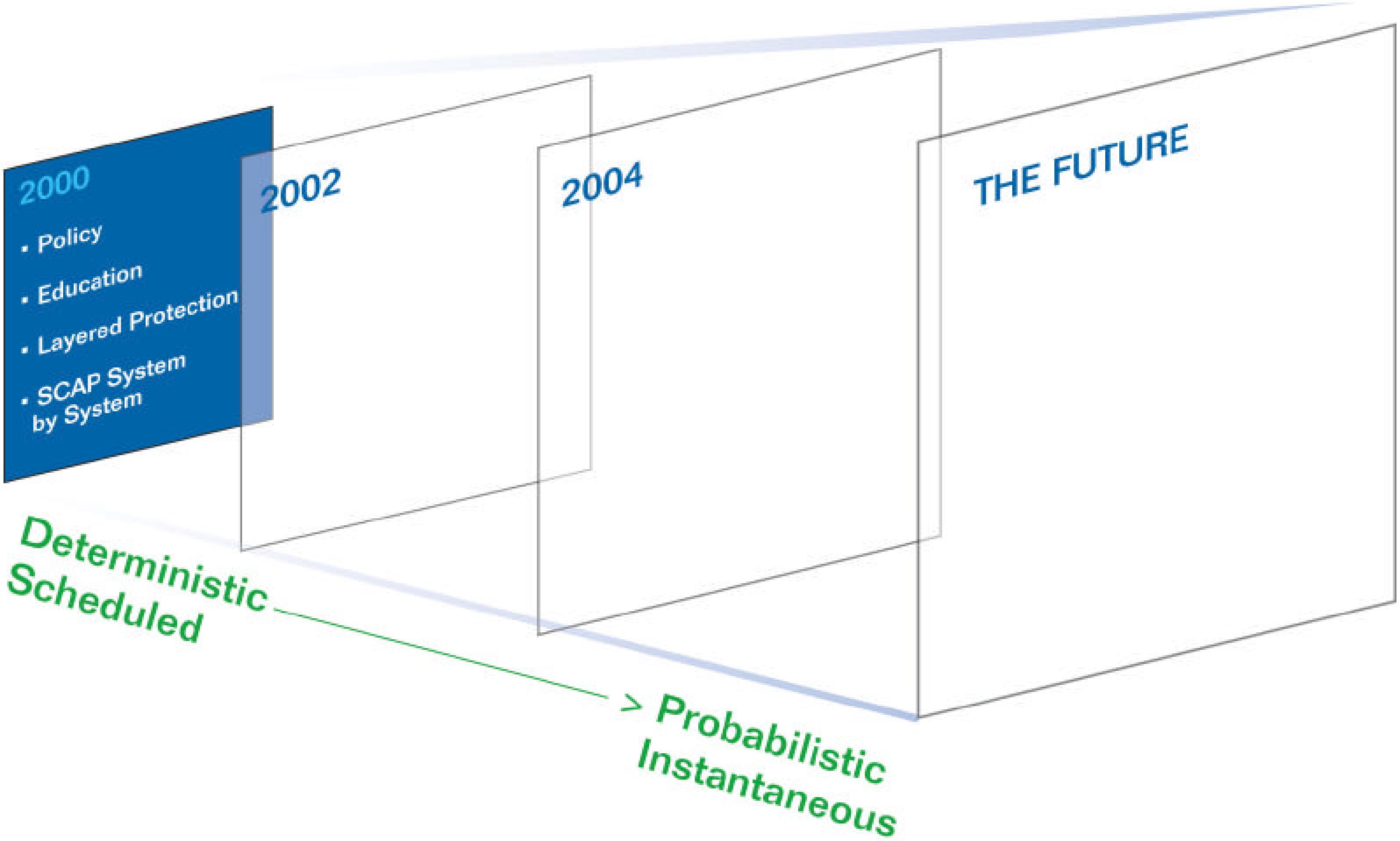
Vulnerable Population Saturation Time

· Code Red	24 hours
Slammer	30 minutes

Decreasing Vulnerability to Exploit Time—

Sometimes less than a day

The Evolving Landscape of Cyber Security



2000

- Policy
- Education
- Layered Protection
- SCAP System by System

2002

2004

THE FUTURE

Deterministic Scheduled > Probabilistic Instantaneous

Policy and Education

Policies are in place to address:

Facility Security Management

Personnel Security Program

Information Systems Security

Internet Access Points and Internet Services

Software Release

Active Training Program:

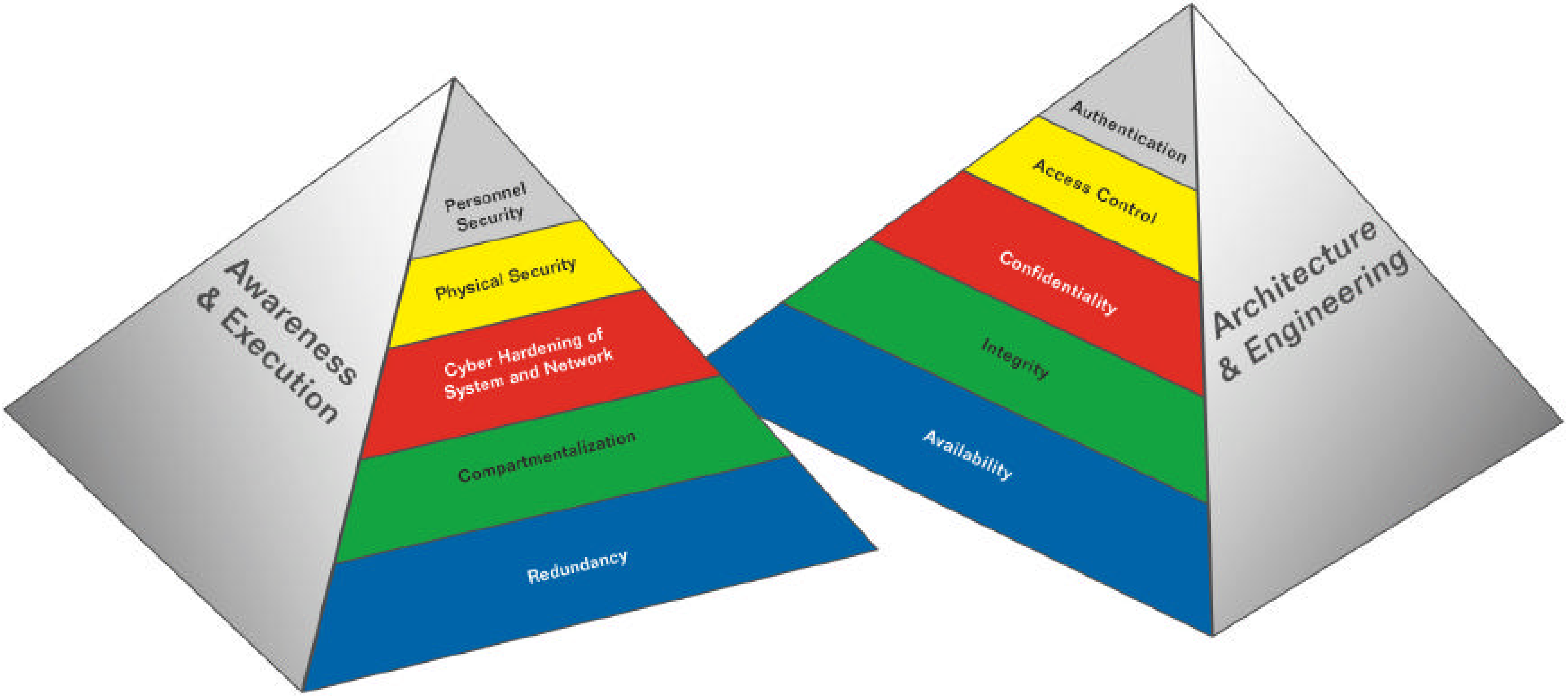
•**FY-00** – Over 40,000 employees viewed 30 minute training video on awareness. Also, 200 employees trained on vulnerability assessment.

•**FY-01** – More than 4,000 employees attended Awareness Day sessions held throughout the FAA. More than 100 employees attended CISSP Training.

•**FY-02** - Delivered Web-based awareness portal and computer-based training. Also deployed mobile training teams.

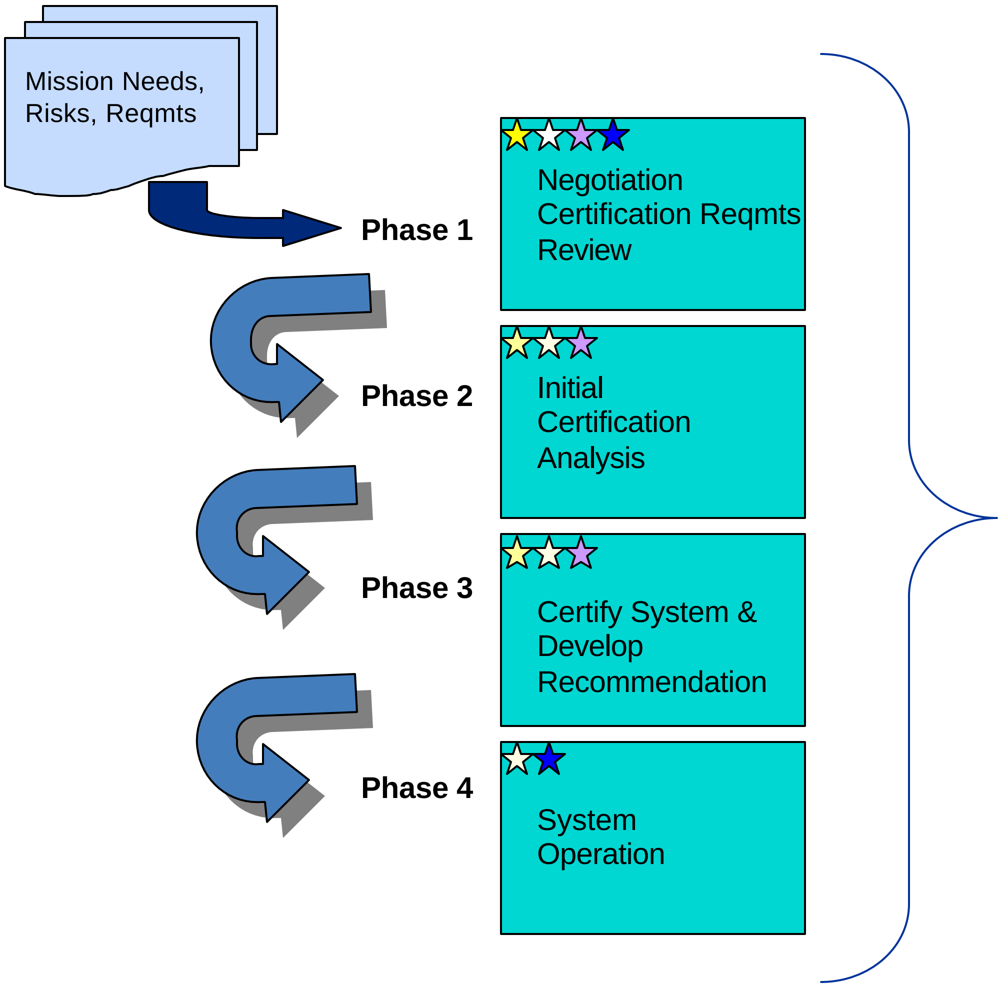
•**FY-03** – More than 600 key personnel being targeted for specialized training; ISS awareness Kiosk traveling to nine Regions and two Centers; continued emphasis on IT curriculum at IRMC and on computer-based training.

FAA's 5 Layers of System Protection



SECURING INDIVIDUAL SYSTEMS

National Information Assurance Certification and Accreditation Program (NIACAP)


Mission Needs, Risks, Reqmts
Phase 1
Negotiation Certification Reqmts Review
Phase 2
Initial Certification Analysis
Phase 3
Certify System & Develop Recommendation
Phase 4
System Operation

☆ Developer

☆ Operator

☆ Certifier

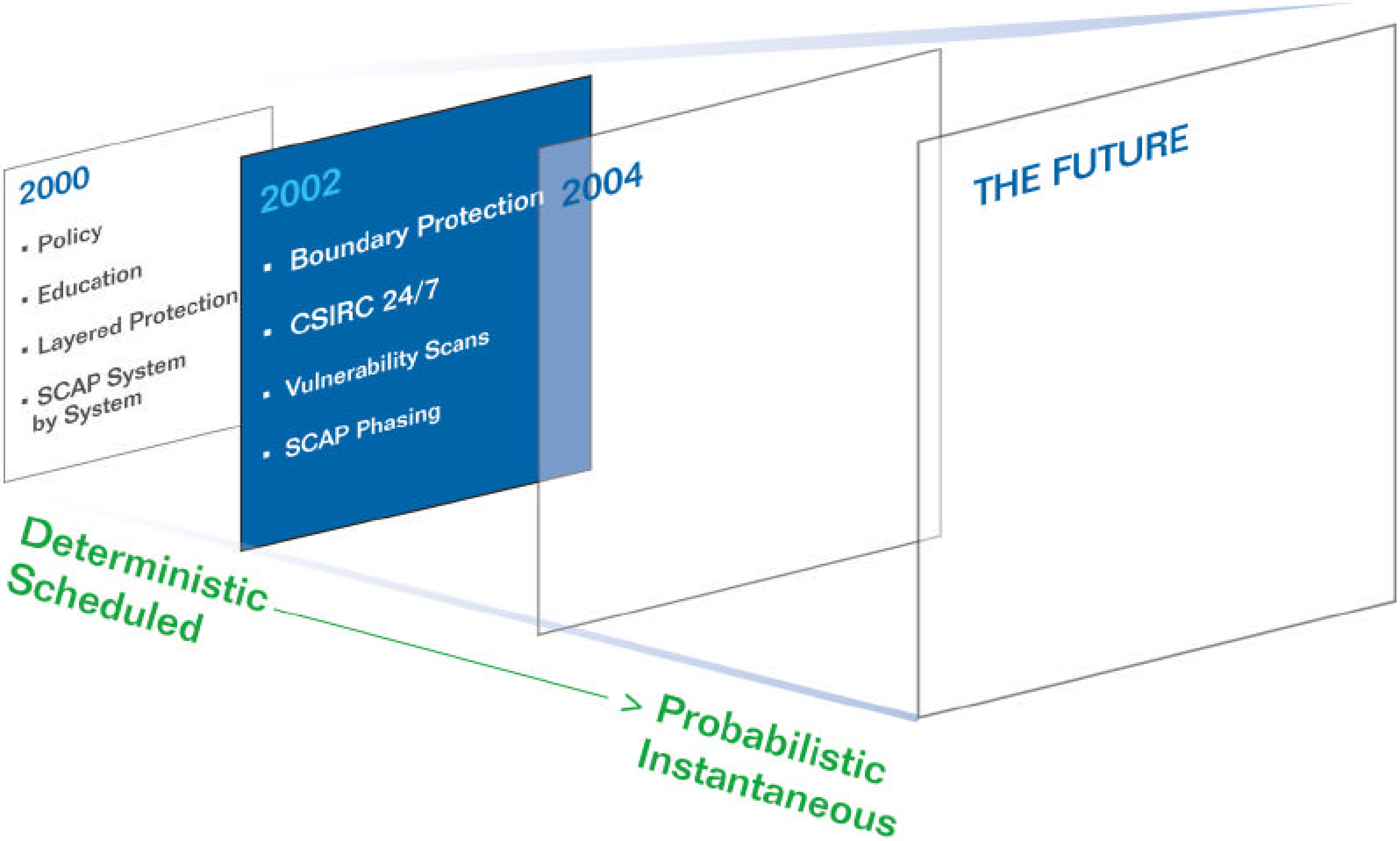
★ User Rep

Nationally Recognized Process

Security Requirements Review During Milestone Zero

Cradle to Grave Program

The Evolving Landscape of Cyber Security



2000

- Policy
- Education
- Layered Protection
- SCAP System by System

2002

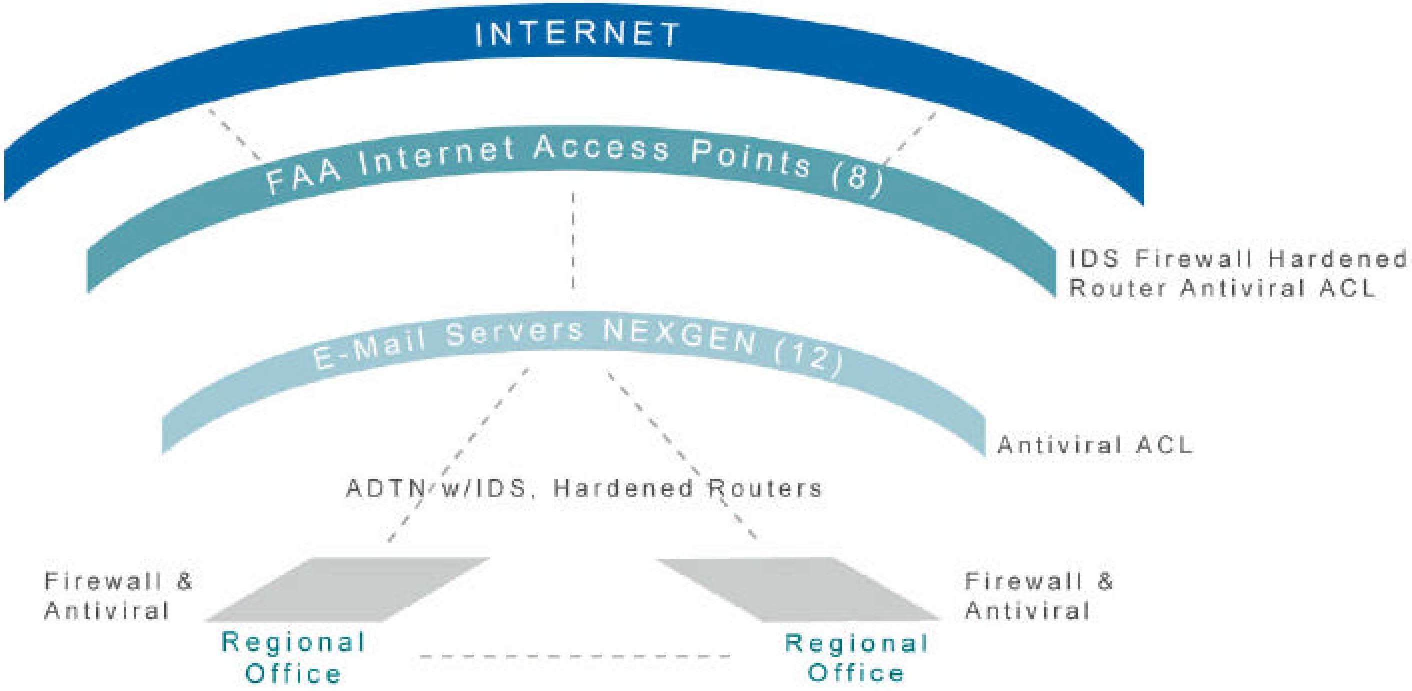
- Boundary Protection
- CSIRC 24/7
- Vulnerability Scans
- SCAP Phasing

2004

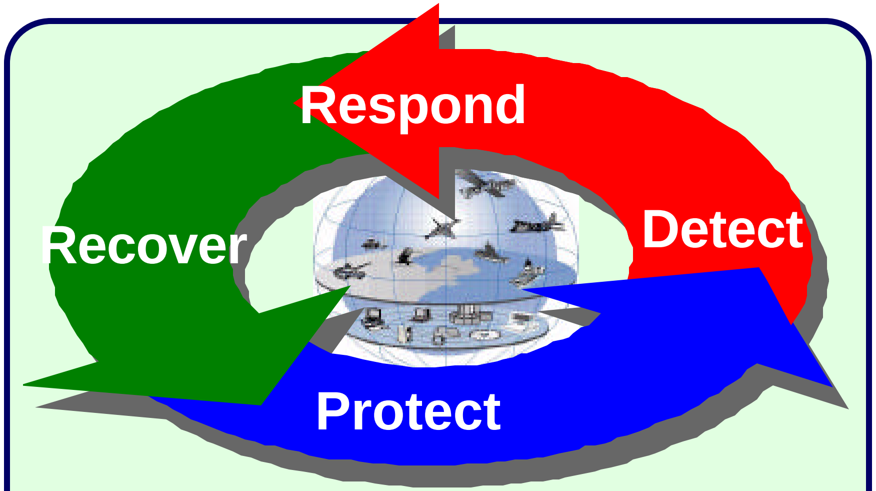
THE FUTURE

Deterministic Scheduled > Probabilistic Instantaneous

Boundary Protection


INTERNET
FAA Internet Access Points (8)
IDS Firewall Hardened Router Antiviral ACL
E-Mail Servers NEXGEN (12)
Antiviral ACL
ADTN w/IDS, Hardened Routers
Firewall & Antiviral
Regional Office
Firewall & Antiviral
Regional Office

Computer Security Incident Response Center (CSIRC)



Protect the information infrastructure

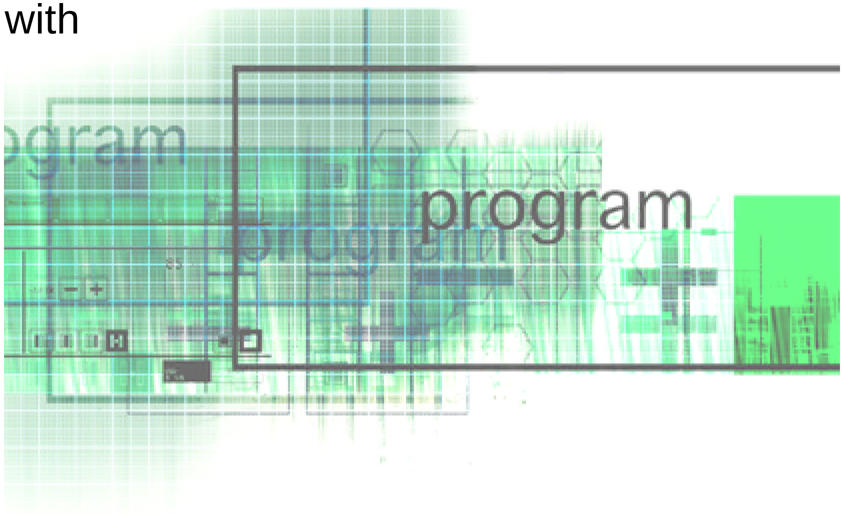
Detect anomalous traffic

Respond to any intrusion that threatens to impede operations

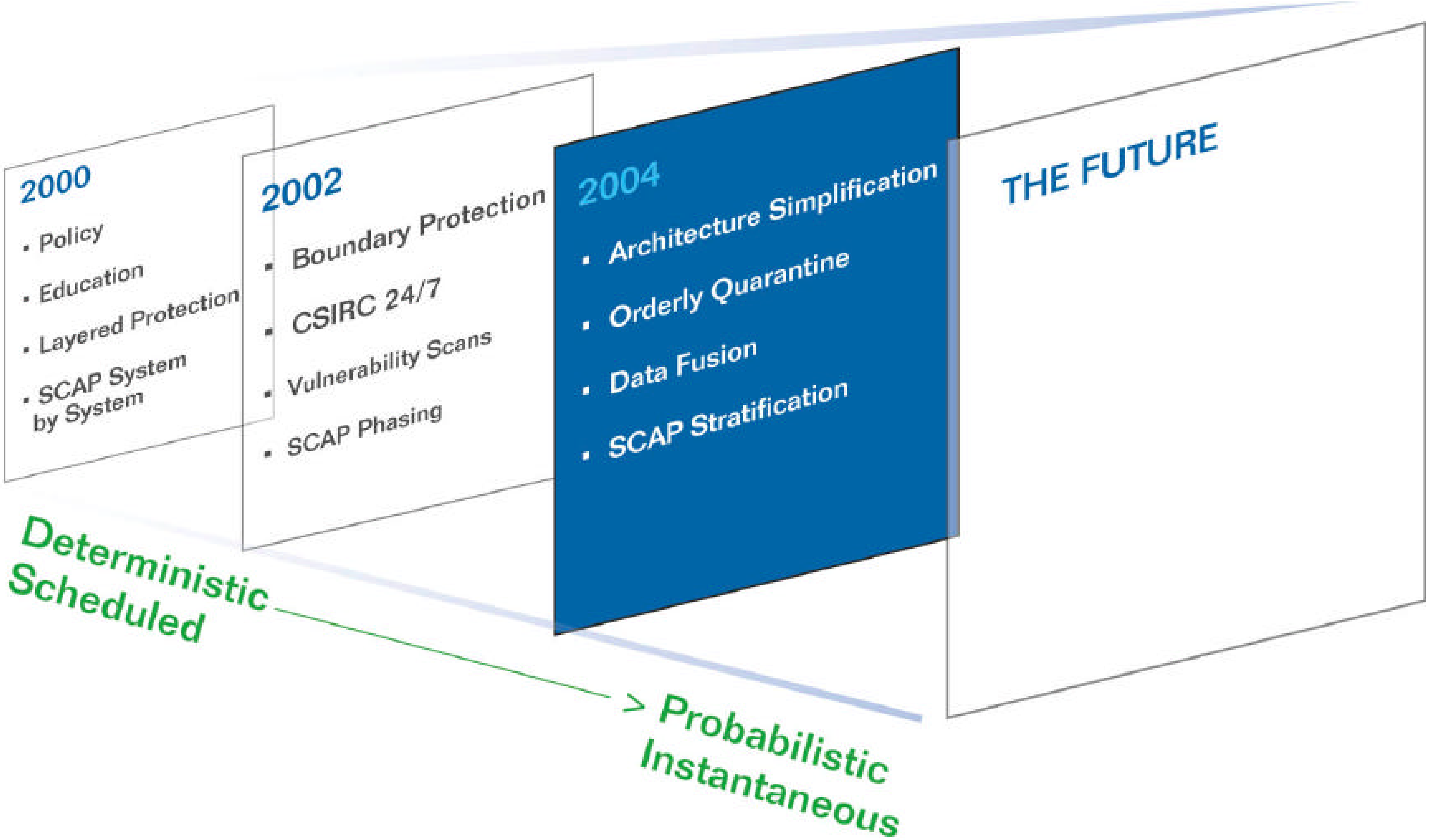
Recover and restore affected systems in a timely fashion

System Compliance Scanning Program

- Scanning tools tuned to “SANS Top 20” – 250 common vulnerability events
- System administrators trained to conduct scanning
- Proactive testing for unremediated vulnerabilities
- Remediation progress being tracked with system administrators



The Evolving Landscape of Cyber Security



2000
- Policy
- Education
- Layered Protection
- SCAP System by System

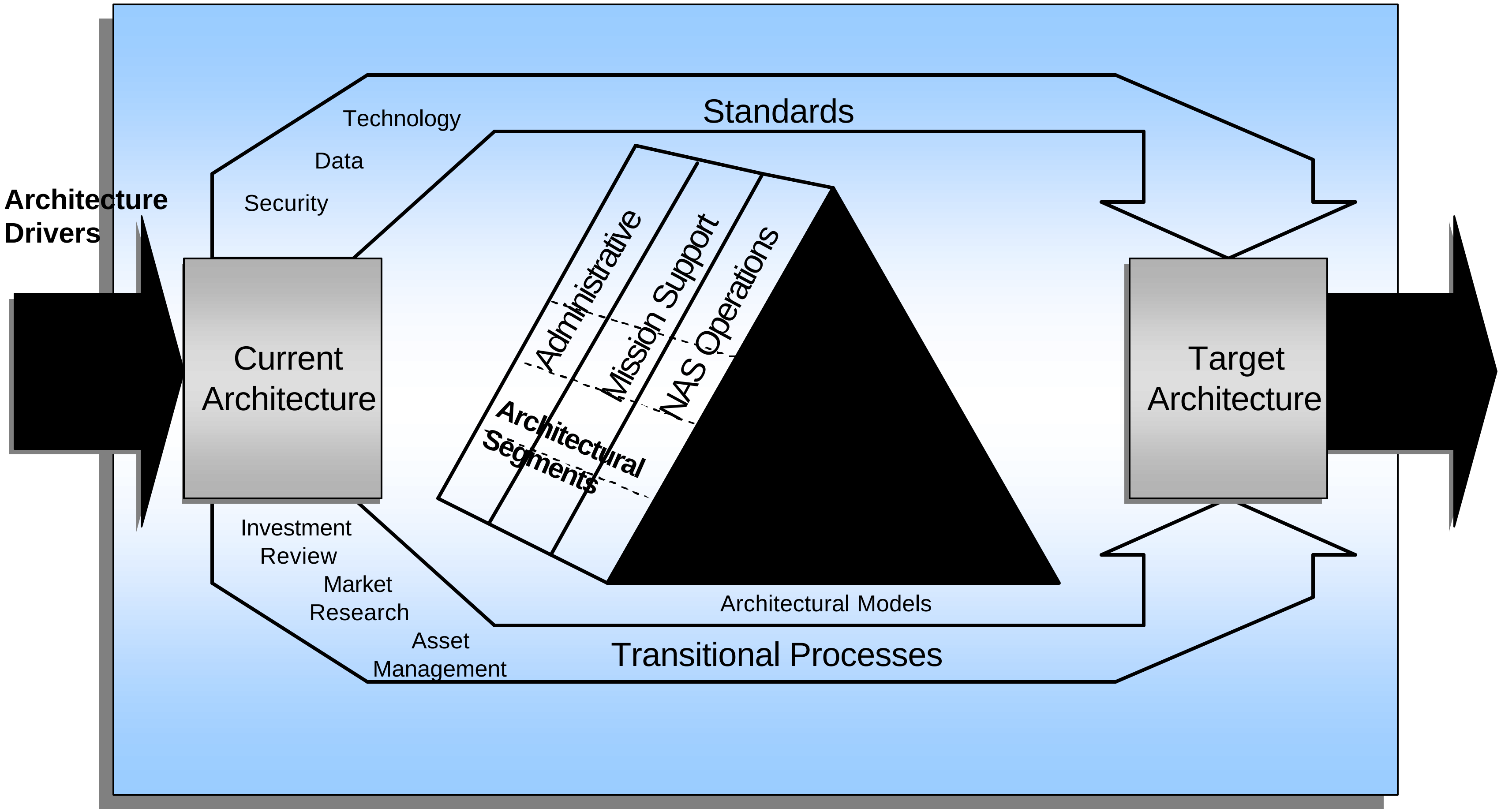
2002
- Boundary Protection
- CSIRC 24/7
- Vulnerability Scans
- SCAP Phasing

2004
- Architecture Simplification
- Orderly Quarantine
- Data Fusion
- SCAP Stratification

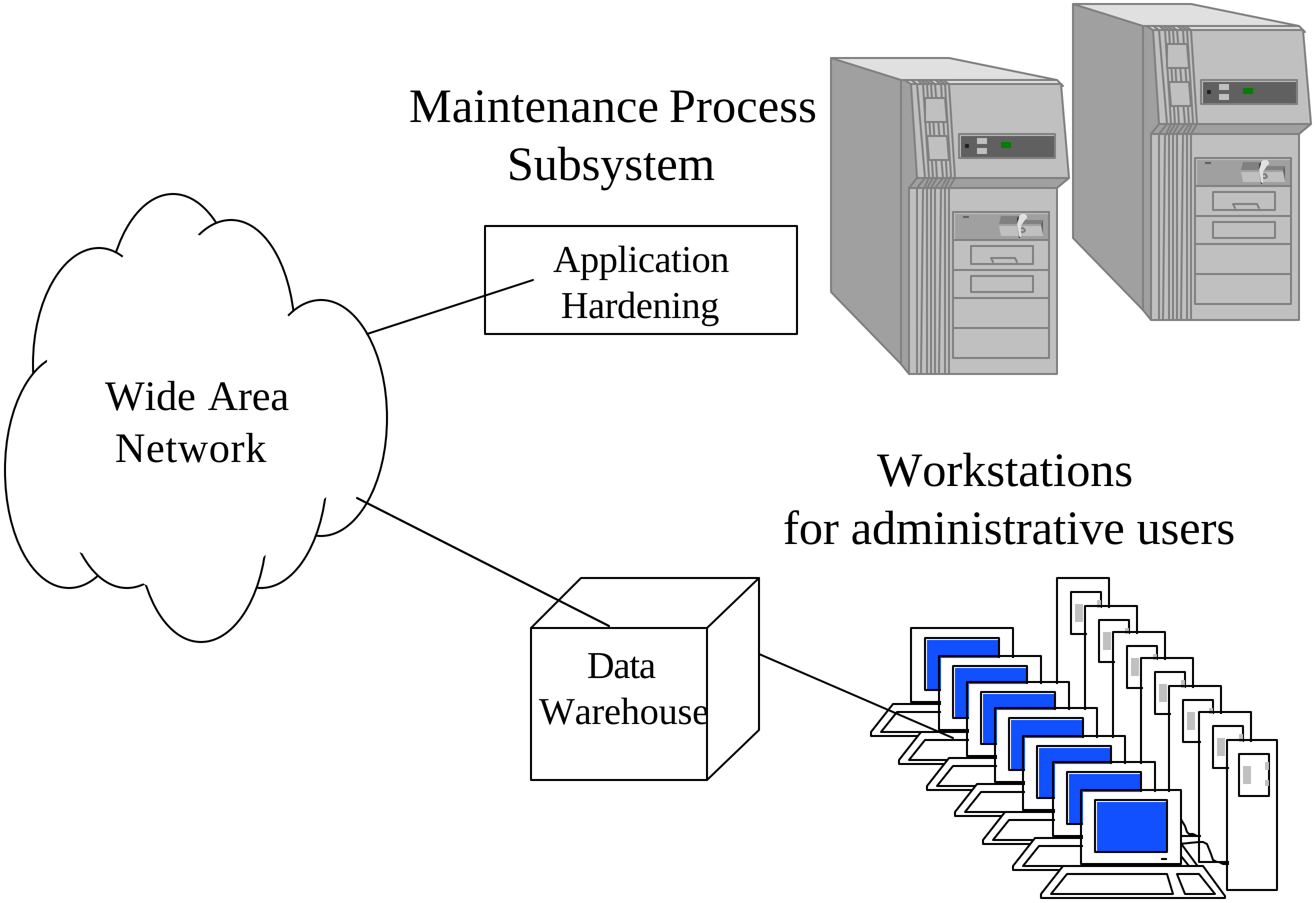
THE FUTURE

Deterministic Scheduled > Probabilistic Instantaneous

Architecture Simplification



Orderly Quarantine
Remote Maintenance Monitoring System



Maintenance Process Subsystem

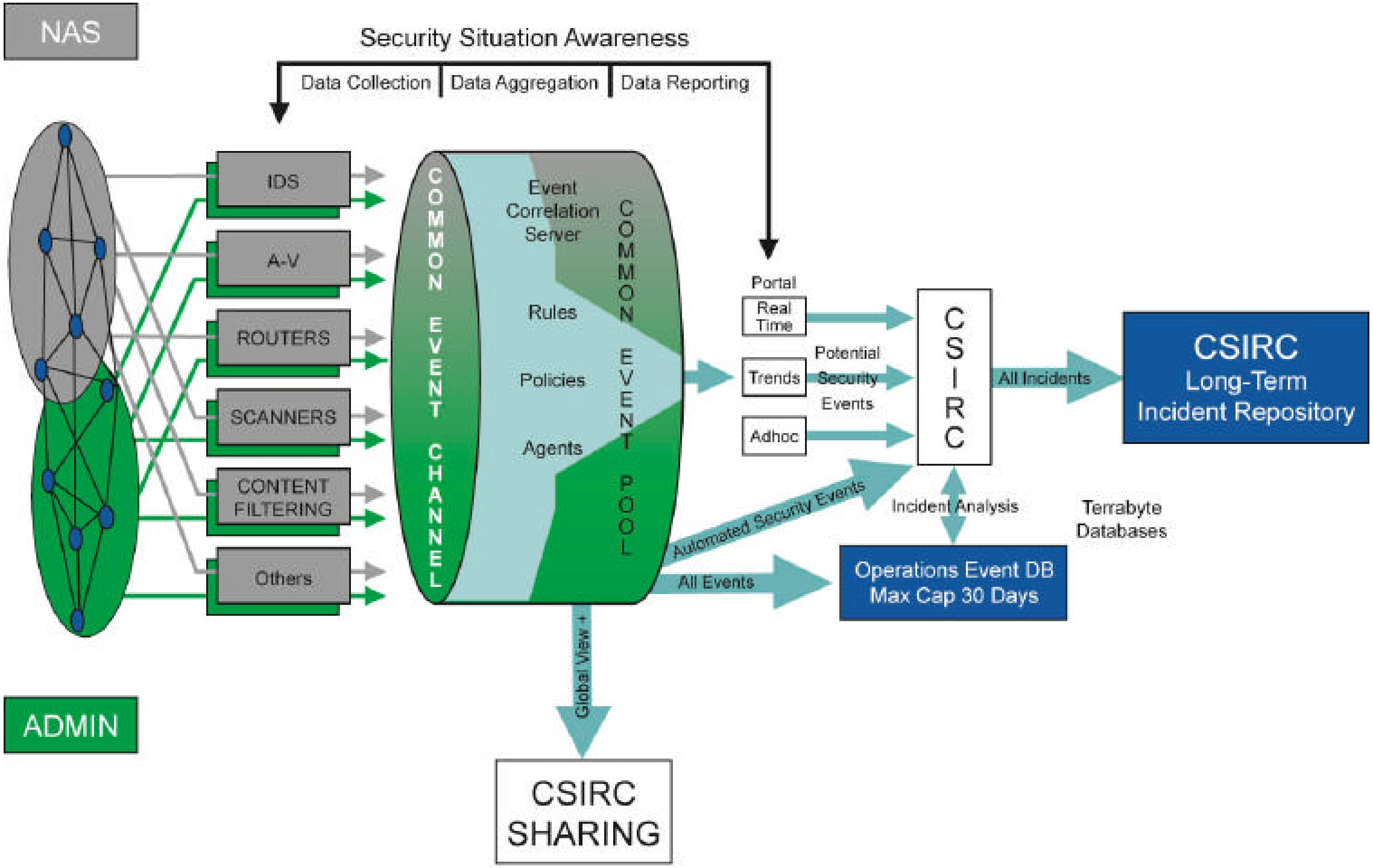
Application Hardening

Wide Area Network

Workstations for administrative users

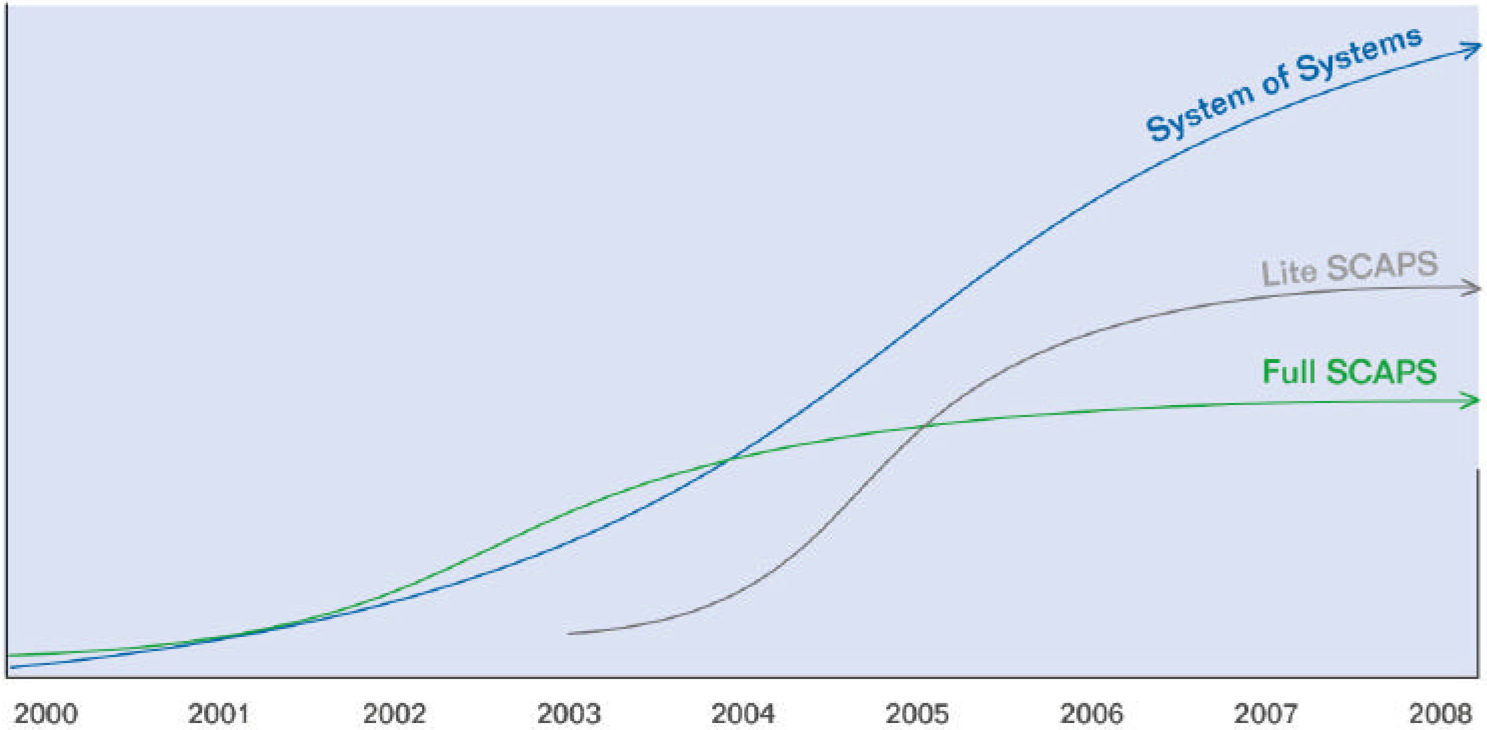
Data Warehouse

Data Fusion and Interpretation



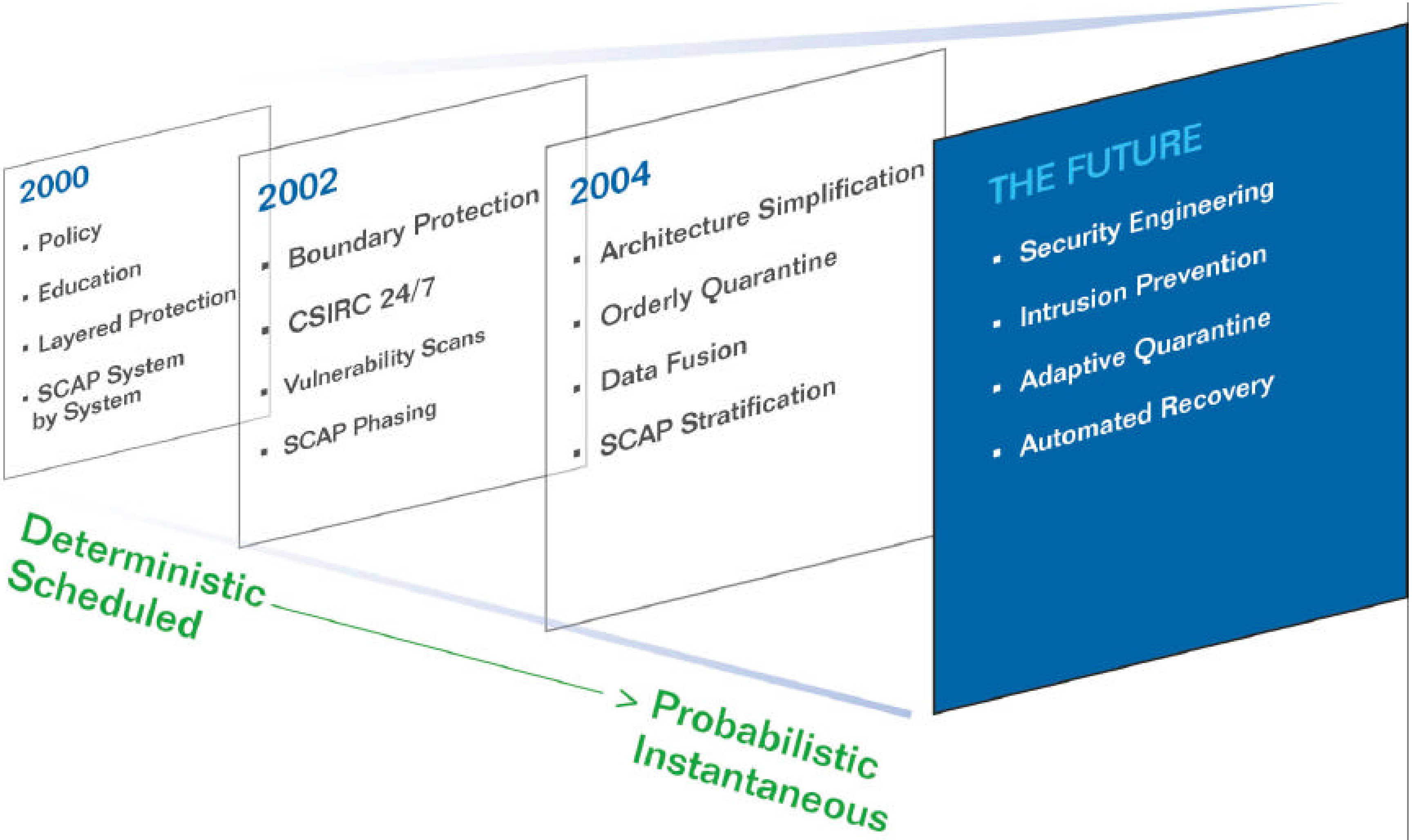
Diagnostic data is from all sources but all traffic is not co-mingled

Reinforcing Protection Mechanisms



Deterministic ——————————> Probabilistic
Scheduled Instantaneous

The Evolving Landscape of Cyber Security



2000

- Policy
- Education
- Layered Protection
- SCAP System by System

2002

- Boundary Protection
- CSIRC 24/7
- Vulnerability Scans
- SCAP Phasing

2004

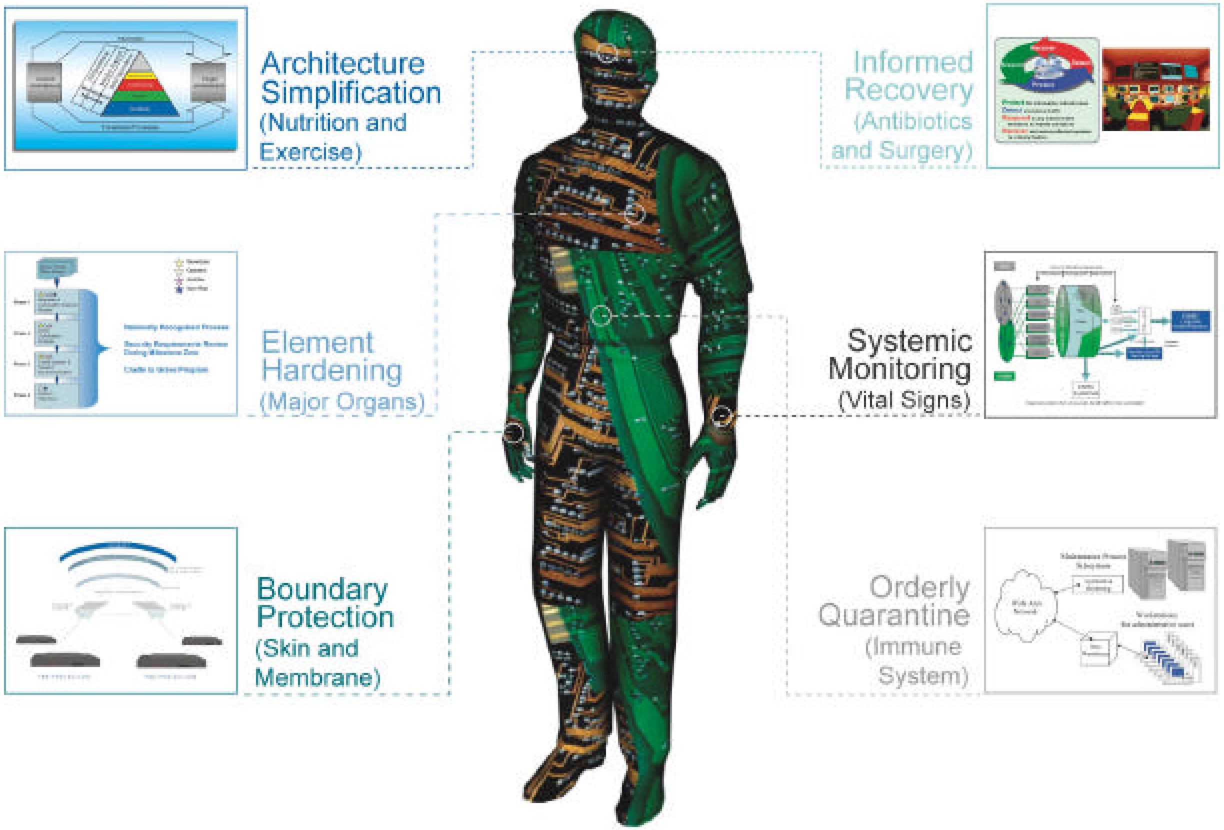
- Architecture Simplification
- Orderly Quarantine
- Data Fusion
- SCAP Stratification

THE FUTURE

- Security Engineering
- Intrusion Prevention
- Adaptive Quarantine
- Automated Recovery

Deterministic Scheduled > Probabilistic Instantaneous

The “Android” Cyber Defense – Emulates the most resilient system in the world



Architecture Simplification (Nutrition and Exercise)

Informed Recovery (Antibiotics and Surgery)

Element Hardening (Major Organs)

Systemic Monitoring (Vital Signs)

Boundary Protection (Skin and Membrane)

Orderly Quarantine (Immune System)

The "Android" Cyber Defense – Areas for Research and Development

- Enhanced methods and standards for engineering security into products and allowing continuous external monitoring of a system's internal "vital signs"

- Improved ability to provide continual security risk assessment in a complex networked environment

- Improved adaptive "quarantine" through provision of dynamically configured "break points" in networks

- Modeling and simulation of heterogeneous networks to quantify tradeoffs between system functionality and security services and to optimi ze "throughput" in the face of latency and highly variable attacks

- Strong identification/authentication mechanisms in bandwidth constrained environments

- Improved methods for testing of security requirements

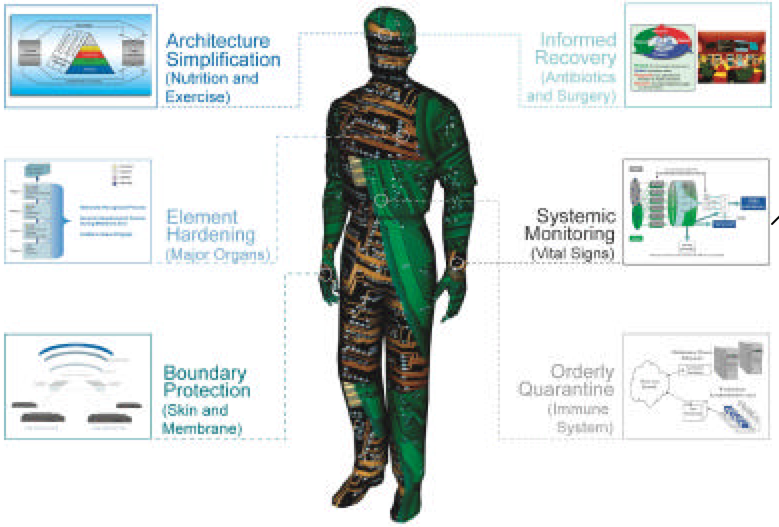
- Role-based network objects and allocation rules

The "Android" Cyber Defense – Areas for Standards Development

Best Practices— Security Engineering

"Efficient" Code Delivery

Improved Requirements and Testing Capability


Architecture Simplification (Nutrition and Exercise)
Element Hardening (Major Organs)
Boundary Protection (Skin and Membrane)
Informed Recovery (Antibiotics and Surgery)
Systemic Monitoring (Vital Signs)
Orderly Quarantine (Immune System)

External Monitoring of Internal Vital Signs

Quarantine Enabling Rules

Cyber Security Key Concepts

- Conventional “defense-in-depth” needs to evolve to an “android” cyber defense because the FAA’s infrastructure is complex and potential attackers can be sophisticated
- The “android” cyber defense blends insights from computer science, health science, and operations research in an attempt to emulate the resilience of the human biosystem
- A robust simplified architecture with multiple layers of protection continues to be a key to success
- The challenge is pervasive and global, requiring constant vigilance and outreach to all segments of the nation’s critical infrastructure, as well as to other nations
- Dynamic network reconfiguration and automated recovery algorithms will be needed for long-term cyber protection
- People and processes must be married with technology and optimized for a successful program
- The National Science Foundation and the American National Standards Institute have important roles in leading research and establishing standards that will enable longer term solutions